# Inadvertent Spoliation of ESI After the 2006 Amendments: The Impact of Rule 37(e)

## Thomas Y. Allman\*

I.	Introduction	25
	A. The Context	26
	1. Scope	27
	2. Routine Operations	28
	3. "Good Faith"	29
	4. Intentional Destruction	31
	5. Exceptional Circumstances	32
	B. Impact of Rule 37(e)	32
	C. Corporate Information Policies	33
	D. Technological Innovation	35
II.	Conclusion	37

#### I. Introduction

Fed. R. Civ. P. 37(e), enacted as part of the 2006 E-discovery Amendments ("the 2006 Amendments"), prohibits the imposition of rule-based sanctions for losses of electronically stored information ("ESI") due to routine operations of information systems which, in retrospect, are judged to have been undertaken in "good faith."

As revised and effective on December 1, 2006, the Rule provides as follows:

"Failure to Provide Electronically Stored Information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a

<sup>\* ©2008</sup> Thomas Y. Allman. Tom Allman, a former General Counsel, was an early advocate of the "safe harbor" e-discovery amendment to the Federal Rules and is an Editor of the Sedona Principles (Second Edition) (2007).

<sup>1.</sup> FED. R. CIV. P. 37(e) (Rule 37(f) was renumbered as Rule 37(e) as part of the 2007 Amendments to the Federal Rules of Civil Procedure (the "style" amendments) and is consistently referred to as Rule 37(e) herein).

result of the routine, good-faith operation of an electronic information system."

To say that Rule 37(e) has been met with intellectual disdain since its enactment is putting it mildly.<sup>2</sup> To many, it evokes "a low standard [which] seems to protect against sanctions only in situations where [they] were unlikely to occur."<sup>3</sup> Moreover, some courts "have completely ignored the clear implication of Rule 37(e) – namely that it applies after the duty to preserve has arisen," thereby "render[ing] the rule largely superfluous."<sup>4</sup>

Accordingly, many commentators have characterized Rule 37(e) as "illusory" and a "safe" harbor in name only. Indeed, the former Chair of the Advisory Committee has rejected the "safe harbor" label. In order to better assess these concerns, we first discuss the key attributes of the Rule and then move to an assessment of its impact on the evolving case law and on corporate retention policies and technology innovation.

#### A. The Context

Rule 37(e) reflects a judgment that "discovery should not prevent continued routine operation of computer systems." As *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, explained, "[Rule 37(e)] recog-

<sup>2.</sup> See, e.g., Oklahoma ex rel. Edmondson v. Tyson Foods, Inc., No. 05-CV-329-GKF-SAJ, 2007 WL 1498973 at \*6 (N.D. Okla. May 17, 2007) (advising the parties that they should be cautious in relying upon any 'safe harbor' doctrine as described in new [Rule 37(e)]).

<sup>3.</sup> Lloyd S. van Oostenrijk, Comment, *Paper or Plastic?: Electronic Discovery and Spoliation In The Digital Age*, 42 Hous. L. Rev. 1163, 1201 (2005). *See*, e.g., Brown v. Chertoff, 563 F.Supp. 2d 1372 (S.D. Ga. 2008) (stating that inadvertent loss of hard copy employment records are subject to sanctions); Whitney v. JetBlue Airways Corp., No. 07-CV-1397 (CBA), 2008 WL 2156324 (E.D.N.Y. April 29, 2008) (stating that careless loss of original note was not sanctioned due to lack of prejudice). *See also* Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 107-08 (2d Cir. 2002) (limiting the impact due to Rule 37(e) when the loss of electronically stored information occurs in the context of a "routine" information system operation, leaving open, in other contexts, the prospect of sanctions for negligent losses of relevant information where prejudice exits).

<sup>4.</sup> Andrew Hebl, Spoliation of Electronically Stored Information, Good Faith, and Rule 37(e), 29 N. Ill. U. L. Rev. 79, 103-04 (Fall, 2008).

<sup>5.</sup> Mark S. Sidoti, *Rule 37(f) – Has This 'Safe Harbor' Provided Any Protection?*, THE AMERICAN LAWYER, Special Sponsor Supplement, Dec. 2007.

<sup>6.</sup> Martin D. Beirne, George B. Murr & and David A. Pluchinsky, *The Illusory Safe Harbor of Rule 37(f)*, The American Lawyer, Corporate Counsel, Dec. 2006.

<sup>7.</sup> See Hon. Lee H. Rosenthal & Hon. James C. Francis IV, Panel Discussion, Managing Electronic Discovery: Views from the Judges, 76 FORDHAM L. REV. 1, 16 (2007) ("Anything that starts with the words 'absent exceptional circumstances' is not a safe harbor.").

<sup>8.</sup> Turner v. Resort Condo. Int'l, LLC, No. 1:03-CV-2025-DFH-WTL, 2006 WL 1990379 at \*6 n.2 (S.D. Ind. July 13, 2006) (refusing sanctions for failure to meet preserva-

nize[s] that suspending or interrupting automatic features of electronic information systems can be prohibitively expensive and burdensome."9

The Civil Rules Advisory Committee acted in response to concerns that the threat of spoliation sanctions for inadvertent losses had caused producing parties to "over-preserve." This was a significant concern, as "many courts have not been hesitant to impose severe sanctions on corporate defendants for the destruction of electronic discovery, even when the loss of discovery is clearly the result of carelessness rather than a desire to hide the truth." Even when the perceived threat proved to be unnecessary, the legacy of over-preservation can be an accumulation of duplicative and irrelevant data that must be reviewed in the event of litigation, making discovery "more expensive and time-consuming." 12

#### 1. Scope

Rule 37(e) applies only to mitigation of "rule-based" spoliation sanctions, despite the fact that sanctions can also be imposed under the inherent power of courts.<sup>13</sup> Some have concluded that this limitation implies approval to avoid the impact of the Rule by simply relying on a court's inherent powers.<sup>14</sup>

tion demands which did not "accommodate the routine day-to-day needs of a business with a complex computer network.").

<sup>9.</sup> Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 624 (D. Colo. 2007).

<sup>10.</sup> See Shira A. Scheindlin & Kanchana Wangkeo, Electronic Discovery Sanctions in the Twenty-First Century, 11 Mich. Telecomm. & Tech. L. Rev 71 (2004) (noting that electronic information is "much more susceptible to unintentional destruction than hard copy documents" and that "businesses have expressed the need for a 'safe harbor' to protect themselves from sanctions for the inadvertent loss of electronic documents.").

<sup>11.</sup> Michael R. Nelson & Mark H. Rosenberg, *A Duty Everlasting: The Perils of Applying Traditional Doctrines of Spoliation to Electronic Discovery*, 12 Rich. J.L. & Tech. 14, 21 (2006).

<sup>12.</sup> Committee on Rules of Practice and Procedure, Summary of the Judicial Conference, at Rules App. C-83 (Sept. 2005) *available at* http://www.uscourts.gov/rules/Reports/ST 09-2005.pdf.

<sup>13.</sup> See Iain D. Johnston, Federal Courts' Authority to Impose Sanctions for Prelitigation or Pre-order Spoliation of Evidence, 156 F.R.D. 313, 315 (1994) ("[T]he two main sources for remedying acts of spoliation are [the Federal Rules] and the courts' inherent authority to sanction.").

<sup>14.</sup> See, e.g., Nucor Corp. v. Bell, 251 F.R.D 191, 197 n.3 (D.S.C. 2008) ("Assuming arguendo that defendant's conduct would be protected under the safe-harbor provision, Rule 37(e)'s plain language states that it only applies to sanctions imposed under [the Federal Rules], [t]hus, the rule is not applicable when the court sanctions a party pursuant to its inherent powers.").

However, as Moore's Federal Practice has suggested, "a court [should not] sanction a party under its inherent authority unless the sanction would be appropriate under [Rule 37(e)]."<sup>15</sup> There is no principled reason to do otherwise, since the "analysis [under Rule 37(e) and under "inherent power"] is essentially the same."<sup>16</sup> In a world where the very act of deletion is integral to normal operations, it is unfair to treat the inadvertent or negligent loss of electronically stored information as indicative of intent to destroy evidence and to thereby infer spoliation.<sup>17</sup>

As pointed out in a recent article, it would be "anomalous to conclude that a good-faith failure to preserve information after a lawsuit is commenced should be afforded greater protection than an identical failure before suit is filed" simply because Rule 37(e) cannot apply to the exercise of inherent power.<sup>18</sup>

#### 2. Routine Operations

Rule 37(e) addresses only the "routine, good-faith" operations of information systems. The definition of "routine," according to Webster, refers to actions taken "according to a standard procedure" or those which are "ordinary." The Committee Note to Rule 37(e) speaks of "the ways in which such systems are generally designed,

<sup>15.</sup> See 7 John K. Rabiej, Moore's Federal Practice, §37A.57 (2008) (stating that courts have traditionally honored the standards prescribed in the federal rules).

<sup>16.</sup> APC Filtration, Inc. v. Becker, No. 07 C 1462, 2007 WL 3046233 at \*3 (N.D. III. Oct. 12, 2007) (quoting Wiginton v. Ellis, No. 02 C 6832, 2003 WL 22439865 at \*3 (N.D. III. Oct. 27, 2003)); Webb v. Dist. of Columbia, 146 F.3d 964, 971 n.15 (D.D.C. 1998) (explaining that considerations for imposing sanctions under Rule 37(b) and inherent power are the same).

<sup>17.</sup> Martin H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561, 621 (2001) ("Electronic evidence destruction, if done routinely in the ordinary course of business, does not automatically give rise to an inference of knowledge of specific documents' destruction, much less intent to destroy those documents for litigation-related reasons."); Henning v. Union Pac. R.R., 530 F.3d 1206, 1220 (10th Cir. 2008) (stating that mere negligence in losing or destroying records does not support an inference of consciousness of a weak case.). *But see* MOSAID Technologies. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 338-39 (D.N.J. 2004) ("Negligent destruction of relevant evidence can be sufficient to give rise to the spoliation inference.").

<sup>18.</sup> Hon. Paul W. Grimm et al, *Proportionality in the Post-Hoc Analysis of Pre-Litigation Preservation Decisions*, 37 U. Balt. L. Rev. 381, 387 (2008) ("Rule 37(e)'s 'safe harbor' should apply by analogy to define pre-litigation preservation conduct that is not directly governed by those Rules.").

<sup>19.</sup> Webster's II New Riverside Dictionary (Rev. ed. 1996); See, e.g., Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (imposing no sanctions for destruction of information pursuant to a document retention policy which occurs "[as] a matter of routine with no fraudulent intent." (emphasis added)).

programmed, and implemented," and the Advisory Committee has given a number of examples from "present" systems.<sup>20</sup>

## 3. "Good Faith"

Rule 37(e) conditions its application on the presence of "good faith" in the operations at issue. The Committee Note to Rule 37(e) does not explicitly define "good faith" other than to speak of what actions may be required<sup>21</sup> or are not permitted.<sup>22</sup> The Note does list some of the "factors that bear on a party's good faith."<sup>23</sup>

The Advisory Committee initially proposed that a party seeking protection under Rule 37(e) show that it took reasonable steps after it knew or should have known of its duty to preserve,<sup>24</sup> which the Advisory Committee subsequently described as "essentially a negligence test."<sup>25</sup> After public hearings, this limitation was dropped, and the standard was broadened to provide protection from sanctions for losses from "routine, good-faith" operations.<sup>26</sup> Thus, a party who negligently

<sup>20.</sup> Committee on Rules of Practice and Procedure, Summary of the Judicial Conference, at Rules App. C-83 (Sept. 2005), available at http://www.uscourts.gov/rules/Reports/ST09-2005.pdf ("[P]rograms that recycle storage media kept for brief periods against the possibility of a disaster that broadly affects computer operations; automatic overwriting of information that has been 'deleted'; programs that change metadata . . . and programs that automatically discard information that has not been accessed within a defined period or that exists beyond a defined period without an affirmative effort to store it for a longer period [as well as] database programs [which] automatically create, discard, or update information without specific direction from, or awareness of, users.").

<sup>21.</sup> FED. R. CIV. P. 37(f) advisory committee's note, (2006) ("A party's intervention to modify or suspend certain features of [the] routine operation to prevent the loss of information, if that information is subject to a preservation obligation.").

<sup>22.</sup> *Id.* "[A] party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve."

<sup>23.</sup> *Id.* (factors include "the steps the party took to comply with a court order or party agreement" in relation to preserving electronic data).

<sup>24.</sup> See Report from Lee H. Rosenthal, Chair, Advisory Committee on Federal Rules of Civil Procedure, to David F. Levi, Chair, Standing Committee on Rules of Practice and Procedure 51-57 (Aug. 3, 2004), available at http://www.uscourts.gov/rules/comment2005/CV Aug04.pdf. ("A court may not impose sanctions under these rules on the [producing] party for failing to provide [ESI] if: (1) the party took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action; and (2) the failure resulted from loss of the information because of the routine operation of the party's electronic information system.").

<sup>25.</sup> See Report from Lee H. Rosenthal, Chair, Advisory Committee on the Federal Rules of Civil Procedure, to David F. Levi, Chair, Standing Committee on Rules of Practice and Procedure 83-84 (May 27, 2004), available at http://www.uscourts.gov/rules/comment 2005/CVAug04.pdf.

<sup>26.</sup> *Id.* at 84-85 (The Committee "revised [the rule] to adopt a culpability standard intermediate between the two published versions.").

executes its preservation obligations "may [still] benefit from the safe harbor, so long as the party acted in good faith."<sup>27</sup>

The absence of "bad faith" plays a decisive role in defining the presence of "good faith."<sup>28</sup> The cases typically hold that "bad faith" is "when a thing is done dishonestly and not merely negligently."<sup>29</sup> Thus, in *Petcou v. C.H. Robinson Worldwide*, the court declined to sanction a failure to interrupt automatic deletion of e-mail because "[i]t does not appear that defendant acted in bad faith in following its established policy for retention and destruction of e-mails."<sup>30</sup>

The ultimate factual issue will often be whether the relevant actors sought to deliberately take advantage of the routine operations when implementing preservation obligations.<sup>31</sup> As a member of the Advisory Committee succinctly stated during the April 2005 meeting of the Advisory Committee, "[G]ood faith . . . assumes [that the party] did not deliberately use the system's routine destruction functions. If you know it will disappear and do nothing, that is not good faith. . .[t]he line is conscious awareness the system will destroy information."<sup>32</sup>

The mere fact that the loss occurs after a preservation duty has already attached is, of course, not decisive.<sup>33</sup> If the operation at issue

<sup>27.</sup> Lloyd S. van Oostenrijk, Comment, *Paper or Plastic?: Electronic Discovery and Spoliation In The Digital Age, supra,* 42 Hous. L. Rev. 1163, 1201 (2005); accord Gal Davidovitch, Comment, *Why Rule 37(e) Does Not Create a New Safe Harbor For Electronic Spoliation,* 38 Seton Hall L. Rev. 1131, 1139 (2008)).

<sup>28.</sup> See 8A Charles Alan Wright, Arthur R. Miller & Richard L. Marcus, Federal Practice & Procedure §2284.1 (3d ed. 2007) (courts should "[start] with existing cases on bad faith in loss of electronically stored information.").

<sup>29.</sup> Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 635 (D. Colo. 2007).

<sup>30.</sup> Petcou v. C.H. Robinson Worldwide, Inc., No. 1:06-CV-2157-HTW-GGB, 2008 WL 542684, at \*3 (N.D. Ga. Feb. 25, 2008) (noting the degree of defendant's culpability is low and the resulting prejudice to plaintiff is relatively minor).

<sup>31.</sup> See Morris v. Union Pac. R.R., 373 F.3d 896, 902 (8th Cir. 2004) ("The inquiry depends in part on corporate policies, but also to some extent on the intent of corporate employees."). See also The Sedona Conference Working Group on Electronic Document Retention & Production, The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, 72 at cmt. 14d (2d ed. 2007) (explaining that good faith in the context of electronic discovery includes an evaluation of whether the electronic process was designed and implemented to meet business and technical needs or with the intent of thwarting discovery).

<sup>32.</sup> Civil Rules Advisory Comm. Minutes, Apr. 14-15, 2005 at 42, *available at* http://www.uscourts.gov/rules/Minutes/CRAC0405.pdf (internal punctuation omitted).

<sup>33.</sup> Peskoff v. Faber, 244 F.R.D. 54, 60 (D.D.C. 2007) (noting that a failure to interrupt an automatic deletion feature after a duty to preserve attached might serve as the basis for a sanction "without offending amended [Rule 37(e)"]), (quoting Disability Rights Council of Greater Washington v. Washington Metro. Transit Auth., 242 F.R.D. 139, 146 (D.D.C. 2007)) (stating that "[Rule 37(e)] does not exempt a party who fails to stop the operation of a

was conducted in "routine, good faith," the exemption applies. In *Greyhound Lines, Inc. v. Wade*, for example, the Court of Appeals for the Eighth Circuit upheld a refusal to sanction for failure to preserve the contents of an electronic control module (ECM) since "[t]he ultimate focus for imposing sanctions for spoliation of evidence is the intentional destruction of evidence indicating a desire to suppress the truth, not the [mere] prospect of litigation."<sup>34</sup> This principle, as represented by Rule 37(e), justifies a more practical view of parties acting in good faith to implement preservation obligations.<sup>35</sup>

#### 4. Intentional Destruction

A party which utilizes a system involving routine destruction for the purpose of eliminating information believed to be disadvantageous is not operating in "good faith." Thus, in *In re Krause*, the court refused to apply Rule 37(e) where information was lost due to "willful and intentional" use of a "GhostSurf" wiping program.<sup>36</sup> This result echoes the prescient comments of Professor Martin H. Redish that "unnecessarily aggressive document destruction" or "intentional destruction of specific documents out of the normal order" would be "entirely unacceptable, for obvious reasons" in regard to any safe harbor that might be drafted.<sup>37</sup>

In some cases, the lack of an intent to destroy evidence obviates the need to even consider the application of Rule 37(e). Thus, in *Toussie v. County of Suffolk*, the court refused to consider sanctions where backup tapes subject to a preservation obligation were recycled in the absence of intentional action.<sup>38</sup> In contrast, in *Connor v. Sun Trust Bank*, the District Judge was convinced that "the only way" that e-mail subject to automatic deletion could have been lost would have been if

system that [is known to be] obliterating information that may be discoverable in litigation").

<sup>34.</sup> Greyhound Lines, Inc. v. Wade, 485 F.3d 1032, 1035 (8th Cir. 2007).

<sup>35.</sup> Andrew Hebl, Spoliation of Electronically Stored Information, Good Faith, and Rule 37(e), supra, 109 n.8 (2008) (criticizing sanctions levied where employer relied upon employees to execute litigation hold).

<sup>36.</sup> United States v. Krause (In re Krause), 367 B.R. 740, 769 (Bankr. D. Kan. 2007).

<sup>37.</sup> Letter from Martin H. Redish, Professor of Law and Pub. Policy, Northwestern. Univ. Sch. of Law, to Lee Rosenthal, Judge. S.D. Tex., at 8 (Dec. 8, 2003), available at http://www.kenwithers.com/rulemaking/civilrules/ed52.pdf. See also Thomas Y. Allman, Safe Harbors and Preservation: A Response, 5 Sedona Conf. J. 117, 117 (2004) ("[S]afe harbor provisions cannot be 'gamed' or 'designed' to cover up or prevent preservation or production of information.").

<sup>38.</sup> Toussie v. Suffolk, No. CV-1-6716(JS) (ARL), 2007 WL 4565160, at \*8-9 (E.D.N.Y. Dec. 21, 2007) (noting the lack of evidence of prejudice).

[a key managerial employee] had deliberately taken advantage of the deletion process in "bad faith."<sup>39</sup>

#### 5. Exceptional Circumstances

The presence of "exceptional circumstances" may tip the balance against the application of Rule 37(e).

The Advisory Committee had in mind the presence of "serious prejudice" to the requesting party in drafting that exclusion.<sup>40</sup> A court in some circumstances may need to provide "remedies to protect an entirely innocent party requesting discovery against serious prejudice arising from the loss of potentially important information."<sup>41</sup>

## B. Impact of Rule 37(e)

A number of cases potentially implicating Rule 37(e) have been resolved since its enactment. By and large, the results in such cases have been consistent with the Rule even when the court did not expressly cite to it.

Thus, in *Escobar v. City of Houston*, the court refused to sanction the Houston Police Department (HPD) for not interrupting its routine policy of overwriting electronic information after ninety days.<sup>42</sup> The court held, citing Rule 37(e), that "sanctions are not appropriate" because, even if the electronic communications were destroyed in the routine operation of the HPD's computer system, "there is no evidence of bad faith in the operation of the system that led to the destruction of the communications." Similarly, the court in *Columbia Pictures Industries v. Bunnell*, applying Rule 37(e), refused to sanction the overwriting of information temporarily residing in RAM where no demand had been made and the need to preserve was not foreseeable.<sup>44</sup>

Courts have also resolved cases consistent with Rule 37(e) involving the routine overwriting or deletion of active information in order to

<sup>39.</sup> Conner v. Sun Trust Bank, 546 F. Supp. 2d 1360, 1377 (N.D. Ga. 2008).

<sup>40.</sup> Comm. On Rule of Practice and Procedure of the Judicial Conference of the U.S., Report of the Civil Rules Advisory Committee 89 (May 27, 2005), *available at* http://www.uscourts.gov/rules/Reports/CV5-2005.pdf.

<sup>41.</sup> *Id*.

<sup>42.</sup> Escobar v. City of Houston, No. 04-1945, 2007 WL 2900581 (S.D. Tex. Sept. 29, 2007).

<sup>43.</sup> *Id.* at \*19

<sup>44.</sup> Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCCX, 2007 WL 2080419 at \*13-15 (C.D. Cal. May 29, 2007), review denied, 245 F.R.D. 443, 445 (C.D. Cal. 2007) (refusing sanctions).

reduce storage requirements<sup>45</sup> and the recycling of backup storage media<sup>46</sup> pursuant to a retention policy or practice. Other decisions have involved the deletion or overwriting of satellite tracking records,<sup>47</sup> video surveillance tapes,<sup>48</sup> the information on laptops of departed employees,<sup>49</sup> chat room conversations,<sup>50</sup> hyperlinked web sites,<sup>51</sup> and screenshots of temporary information.<sup>52</sup>

An earlier version of Rule 37(e) was used to resolve (and reject) a request for sanctions in regard to "ephemeral" oscilloscope readings.<sup>53</sup>

# C. Corporate Information Policies

Rule 37(e) implicitly validates the use of reasonable corporate policies which are implemented in good faith. The regular purging of electronic data is "necessary to prevent a build-up of data that can overwhelm the most robust electronic information systems."<sup>54</sup> Rule 37(e) clarifies that losses resulting from routine steps undertaken pursuant to a "neutral policy" are presumed to be appropriate even when a general duty to preserve exists.<sup>55</sup>

45. *See Petcou* at \*3 (refusing spoliation instruction); Clearone Commc'n, Inc., v. Chiang, No. 2:07 CV 37 TC, 2008 WL 704228, at \*5 (D. Utah Mar. 10, 2008) (granting spoliation instruction); *Connor*, 546 F. Supp. 2d at 1377 (spoliation instruction granted).

46. See In re Kmart Corp., 371 B.R. 823 (Bankr. N.D. Ill. 2007) (refusing spoliation instruction); Treppel v. Biovail Corp., 249 F.R.D. 111, 124 (S.D.N.Y. 2008) (refusing spoliation instruction but authorizing forensic examination).

47. See Henning v. Union Pac. R.R. Co., 530 F.3d 1206, 1220 (10th Cir. 2008) (refusing spoliation instruction); Ogin v. Ahmed, 563 F. Supp. 2d 539 (M.D. Pa. 2008) (granting spoliation instruction); Greyhound Lines, Inc. v. Wade, 485 F.3d 1032 (8th Cir.2007) (affirming refusal of spoliation sanctions); Frey v. Gainey Transp. Serv., No. 1:05-CV-1493-JOF, 2006 WL 2443787 (N.D. Ga. Aug. 22, 2006) (refusing spoliation instruction).

48. See Mazloum v. D.C. Metro. Police Dep't, 530 F. Supp. 2d 282 (D.D.C. 2008) (granting spoliation instruction); Kounelis v. Sherrer, 529 F. Supp. 2d 503 (D.N.J. 2008) (granting spoliation instruction).

49. See Land O'Lakes, 244 F.R.D. at 638 (refusing spoliation instruction while granting monetary sanctions).

50. Malletier v. Dooney & Bourke, Inc., No. 04 Civ.5316 RMB MHD, 2006 WL 3851151 (S.D.N.Y. Dec. 22, 2006) (denying sanctions regarding discovery and preservation of chat room e-mails).

51. Phillips v. Netblue, Inc., No. C-05-4401 SC, 2007 WL 174459 (N.D. Cal. Jan. 2, 2007).

52. Healthcare Advocates v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 642 (E.D. Pa. 2007) (rejecting spoliation instruction).

53. Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 177 n.4 (S.D.N.Y. 2004) (alluding to issues involving the use of Instant Messenger functions).

54. Roland C. Goss, Hot Issues in Electronic Discovery: Information Retention Programs and Preservation, 42 Tort Trial & Ins. Prac. L.J. 797, 806 (2006).

55. United States v. O'Keefe, 537 F. Supp. 2d 14, 22 (D.D.C. 2008) (stating that Rule 37(e) is the "analogue" of the principle in criminal law that destruction of evidence pursuant to a neutral policy and without evidence of bad faith does not violate due process).

Drafting and implementing corporate information policies is not for the faint of heart. There is no consensus, for example, on how much electronic information to retain and for how long to retain it. A Task Force of the Sedona Conference® Working Group on the retention of e-mail was unable to identify a consensus on the best practices on that topic, either by industry or entity size.<sup>56</sup> Indeed, review indicated that the same entities had successfully adopted, *albeit* at different times in their evolution, quite inconsistent approaches.

As the Supreme Court has noted, document management policies, which are "common in business," appropriately authorize deletion of information when a person "does not have in contemplation any particular official proceeding in which those documents might be material." Commentators recommend "creation, implementation and management of [a] records management policy," coupled with a Litigation Response Plan which allows a party to quickly identify, capture, and preserve potentially relevant records in good faith. 58

However, any policy must be carefully drawn and consistently applied to avoid any inference that it is not routinely applied in good faith. <sup>59</sup> In *Doe v. Norwalk Community College*, poorly executed policies led to ineligibility for Rule 37(e). <sup>60</sup> The court found that e-mail backup tapes were not consistently retained for fixed periods and that a state policy governing retention of communications was not followed. <sup>61</sup> Similarly, a policy cannot be used as a pretext for deliberate destruction of information. In *Doctor John's, Inc. v. Sioux City, Iowa*, a court found it "laughable and frivolous" to argue that the destruction of the

<sup>56.</sup> Sedona Conference Commentary on E-mail Management: Guidelines for the Selection of Retention Policy (Thomas Y. Allman, ed., 2007), 8 Sedona Conf. J. 239 (2007), available at http://www.csueastbay.edu/its/icshm/uit/docs/emailmgmt.pdf.

<sup>57.</sup> Arthur Andersen, LLP v. United States, 544 U.S. 696, 704-08 (2005) (reversing conviction).

<sup>58.</sup> Kevin F. Brady, What Protection Does 37(f) Provide: Is it Meant to be a "Safe Harbor" or a "Lighthouse"?, The Legal Intelligencer, June 11, 2007, E-Evidence Supplement, at EE7, available at http://www.cblh.com/files/BradyLegalIntelligencerJune2007. pdf; See also In re Kmart Corp., 371 B.R. 823 (Bankr. N.D. Ill. 2007) (deletion of e-mail pursuant to existing policy was held to be appropriate because it was not known that discoverable information existed among e-mail being destroyed).

<sup>59.</sup> See Ralph Losey, Rule 37(f) Safe Harbor Requires Routines That Most Companies Lack (noting when written policies are not uniformly followed, courts will look to actual practices to determine what is "routine, good faith" thus making it hard for companies to take advantage of Rule 37(e)), available at http://ralphlosey.wordpress.com/2007/03/03/rule-37f-safe-harbor-requires-routines-that-most-companies-lack/.

<sup>60.</sup> See Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372 (D. Conn. 2007).

<sup>61.</sup> Id. at 378.

only tape recording of a crucial city council meeting was excused by a policy permitting destruction of such information.<sup>62</sup>

#### D. Technological Innovation

There are a number of technological changes on the horizon, such as replacing tape-based backup by disk-based technologies,<sup>63</sup> converting voicemail to e-mail or e-mail attachments,<sup>64</sup> searching backup tapes without restoring their contents,<sup>65</sup> and the use of clustering and other advanced search and retrieval techniques. Rule 37(e), which is technology neutral, will thus help relieve some of the anxiety that plans for innovative information systems may otherwise engender.<sup>66</sup>

Courts are suspicious of innovations which seem to encourage deletion. In *Clearone Communications, Inc. v. Chiang*,<sup>67</sup> the court criticized an e-mail system that did not retain copies of e-mail sent by a party as "a significant irregularity; almost unimaginable for a technology company; and even more unlikely for a person of [the party's] importance in such a company."<sup>68</sup> In *Zurich American Insurance Co. v. Ace American Reinsurance Co.*, the court suggested it had "little sympathy for utilizing an opaque data storage system, particularly when, by the nature of its business, [a potential producing party] can reasonably anticipate frequent litigation."<sup>69</sup> Other courts have penalized choices

<sup>62.</sup> Doctor John's, Inc. v. City of Sioux City, Iowa, 486 F. Supp. 2d 953, 956 (N.D. Iowa 2007).

<sup>63.</sup> Shamus McGillicuddy, *Law Firm Finds Tape Unreliable, Switches to Disk*, Sept. 19, 2007, http://searchcio-midmarket.techtarget.com/news/article/0,289142,sid183\_gci1272977,00. html.

<sup>64.</sup> *Save All*, Waters Financial Technology Intelligence, June 1, 2005, http://db.riskwaters.com/public/showPage.html?page=281113.

<sup>65.</sup> See Index Engines, Automated Offline Tape Discovery (2008), http://www.indexengines.com/download/IE\_Offline\_Tape\_Indexing\_DS.pdf.

<sup>66.</sup> See Timken Co. v. United States, 659 F. Supp. 239, 243 (Ct. Int'l Trade 1987) (rejecting argument that having foreign exporters submit computer tapes would force them into "archaic business practices" to avoid that duty).

<sup>67.</sup> Clearone Commc'ns, Inc. v. Chiang, No. 2:07 CV 37 TC, 2008 WL 704228 (D. Utah Mar. 10, 2008).

<sup>68.</sup> Id. at \*4.

<sup>69.</sup> Zurich Am. Ins. Co. v. Ace Am. Reinsurance Co., No. 05 Civ. 9170 RMB JCF, 2006 WL 3771090 at \*2 (S.D.N.Y. Dec. 22, 2006).

to store information in an inaccessible source<sup>70</sup> or to decommission a system once a preservation obligation attaches.<sup>71</sup>

However, as early as 1978, the U.S. Supreme Court in *Oppenhemier Fund, Inc. v. Sanders* stated that it "borders on the frivolous" to argue that a party should be penalized for not keeping its records "in the form most convenient to some potential future litigants whose identity and perceived needs could not have been anticipated."<sup>72</sup> More recently, a court refused to require a party to create a business process to preserve temporary communications posted in chat rooms where there was no current business process or requirement.<sup>73</sup> Similarly, courts have refused to require parties to install mechanisms to record oscilloscope readings, <sup>74</sup> hyperlinked websites, <sup>75</sup> or screenshots.<sup>76</sup>

Certainly there is a need for skepticism regarding overt attempts to prospectively interfere with preservation of relevant information. However, absent evidence of deliberate intent to evade known duties, "[i]nevitably and by their nature, electronic storage platforms and media will come and go, a fact that should be considered by courts" in assessing these types of issues.<sup>77</sup>

As *Sedona Principle* Six notes, "[r]esponding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronic data and documents."<sup>78</sup>

<sup>70.</sup> Quinby v. WestLB AG, No. 04Civ. 7406(WBP)(HBP), 2005 WL 3453908, at \*8 n.10 (S.D.N.Y. Dec. 15, 2005) (holding no sanctions for moving e-mail to backup media from active media, but did decline to shift the costs of restoring e-mail from the inaccessible media).

<sup>71.</sup> Xpedior Creditor Trust v. Credit Suisse First Boston (USA), Inc., 309 F. Supp. 2d 459, 465 (S.D.N.Y. 2003) (rendering computer files inaccessible by virtue of the decommissioning of the systems).

<sup>72.</sup> Oppenhemier Fund, Inc. v. Sanders, 437 U.S. 340, 363 (1978).

<sup>73.</sup> Malletier v. Dooney & Bourke, Inc., No-04-Civ. 5316(RMB)(MHD), 2006 WL 3851151, at \*2 (S.D.N.Y. Dec. 22, 2006).

<sup>74.</sup> Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 177 (S.D.N.Y. 2004).

<sup>75.</sup> Phillips v. Netblue, Inc., No. C054401(SC), 2007 WL 174459 (N.D. Cal. Jan. 22, 2007).

<sup>76.</sup> Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 642 (E.D. Pa. 2007).

<sup>77.</sup> Mia Mazza, Emmalean K. Quesada, Ashley L. Sternberg, *In Pursuit of FRCP 1: Creative Approachres to Cutting and Shifting the Costs of Discovery of Electronically Stored Information*, 13 Rich. J.L. & Tech. 11, 147-48 (2007), *available at* http://law.richmond.edu/jolt/v13i3/article11.pdf ("businesses should be free to change information systems without being penalized in later litigation.").

<sup>78.</sup> The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, The Sedona Conf., Jan. 2004, at 27, available at http://thesedonaconference.org/content/miscFiles/publications\_html.

#### II. CONCLUSION

Rule 37(e) was intended to suggest that spoliation of electronically stored information should be assessed by a flexible standard which turns on the manifested intent of the participants in the operations involved.<sup>79</sup> The mere fact that a duty to preserve can be identified as in effect at the time of the loss should not be the sole determining factor where no intent to evade litigation responsibilities is shown.

With some exceptions, the Rule has succeeded in making this point, albeit not without some resistance from a few courts. Rule 37(e) has served as a useful guidepost for assessing compliance with preservation obligations in the context of electronic information. It "contemplate[s] that the parties will act in good faith in the preservation and production of documents,"80 and courts at all levels have rejected "exaggerated sanction claims unless there has been a deliberate manipulation of systems."81

Thus, even if it were true that "Rule 37(e) [does] not, in most cases, offer any protection that the Federal Rules did not already provide," there is, as a member of the Advisory Committee noted at the time, a "real benefit in reassuring parties that if they respond to [challenges] reasonably, they will be protected." 83

<sup>79.</sup> Thomas Y. Allman, Rule 37(f) Meets Its Critics: The Justification for a Limited Preservation Safe Harbor for ESI, 5 Nw. J. Tech. & Intell. Prop. 1, 5 (2006).

<sup>80.</sup> Texas v. Citry of Frisco, No. 4:07cv383, 2008 WL 828055 (E.D. Tex. Mar. 27, 2008) (encouraging potential adversaries to "handle the preservation of documents in response to their respective litigation holds in such good faith").

<sup>81.</sup> Hon. Lee Rosenthal, quoted in Jason Krause, *E-Discovery Tips From the Bench*, Law.comNewswire, June16, 2008, http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202422260266.

<sup>82.</sup> Gal Davidovitch, Comment, Why Rule 37(e) Does Not Create a New Safe Harbor For Electronic Spoliation, 38 Seton Hall L. Rev. 1131, 1131 (2008) (arguing that even though Rule 37(e) is ineffective, the fact that some might think it is effective may lead them to try to use it to commit acts ("untoward reactions") they should not undertake).

<sup>83.</sup> See Civil Rules Advisory Committee Minutes, April 15-16, 2004, at 20, available at http://www.uscourts.gov/rules/Minutes/CRAC0404.pdf.